Discrete Structures	*Prelim 1 sample questions—* ***Solutions***
CS2800	*Selected problems from past exams*

1. *True/false. For each of the following statements, indicate whether the statement is true or false. Give a one or two sentence explanation for your answer.*

   (a) *A proof that starts "Choose an arbitrary $y \in \mathbb{N}$, and let $x = y^2$" is likely to be a proof that $\forall y \in \mathbb{N}, \forall x \in \mathbb{N}, \dots$.*

   Solution False. This would only be a proof that $\exists x \in \mathbb{N}$ with some property, not a proof that $\forall x \in \mathbb{N}$ the property holds.

   (b) *The set of real numbers ($\mathbb{R}$) is countable.*

   Solution False. We proved this in class using diagonalization.

   (c) *The set of rational numbers ($\mathbb{Q}$) is countable.*

   Solution True. We proved this in class by giving a procedure for listing all of the rational numbers (by putting them in a table and traversing the diagonals of the table).

   (d) *Recall that $[X \to Y]$ denotes the set of functions with domain X and codomain Y. Let $f : 2^S \to [S \to \{0, 1\}]$ be given by $f : X \mapsto h$ where $h : S \to \{0, 1\}$ is given by $h : s \mapsto 0$. f is one-to-one.*

   Solution False. f always returns the same thing, so it can't be one to one. For example, choose any two different subsets X_1 and X_2 of S; then $f(X_1) = h = f(X_2)$.

   (e) *f as just defined is onto.*

   Solution False. Choosee any function $h' : S \to \{0, 1\}$ other than h. Since f only outputs h, it never outputs h'.

2. *Prove the following claim using induction: for any $n \geq 0$, $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$*

   Solution Base case: when $n = 0$, the left hand side is $2^0 = 1$ and the right hand side is $2^2 - 1 = 1$, and they are clearly the same.

   Inductive step: Choose an arbitrary n and assume that $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ (this is the inductive hypothesis).

   We wish to show that $\sum_{i=0}^{n+1} 2^i = 2^{n+2} - 1$. We compute:

$$\begin{aligned}
\sum_{i=0}^{n+1} 2^i &= \sum_{i=0}^{n} 2^i + 2^{n+1} && \text{arithmetic} \\
&= (2^{n+1} - 1) + 2^{n+1} && \text{by the inductive hypothesis} \\
&= 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1
\end{aligned}$$

   as required.

3. *Complete the following diagonalization proof:*

   Claim: *$X = [\mathbb{N} \to \mathbb{N}]$ is uncountable.*

   Proof: *We prove this claim by contradiction. Assume that X is countable. Then there exists a function F :* ***FILL IN*** *that is* ***FILL IN****.*

   Write $f_0 = F(0)$, $f_1 = F(1)$, and so on. We can write the elements of X in a table:

	0	*1*	*2*	$\cdots$
f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$\cdots$
f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\ddots$

   Let f_D : ***FILL IN*** *be given by $f_D : x \mapsto$* ***FILL IN***

   Then ***FILL IN***

   This is a contradiction because ***FILL IN****.*

   Solution **Claim:** $X = [\mathbb{N} \to \mathbb{N}]$ is uncountable.

   Proof: We prove this claim by contradiction. Assume that X is countable. Then there exists a function $F : \mathbb{N} \to X$ that is **onto**.

   Write $f_0 = F(0)$, $f_1 = F(1)$, and so on. We can write the elements of X in a table:

	0	1	2	$\cdots$
f_0	$f_0(0)$	$f_0(1)$	$f_0(2)$	$\cdots$
f_1	$f_1(0)$	$f_1(1)$	$f_1(2)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$		$\ddots$

   Let $f_D : \mathbb{N} \to \mathbb{N}$ be given by $f_D : x \mapsto 1 + f_x(x)$

   Then f_D **is not in the table, because for any i, it differs from f_i on input i.**

   This is a contradiction because **we assumed F was onto**.

4. *Compute $10101b + 101b$ (recall that b indicates the strings of digits should be interpreted as integers using the binary representation). Express your answer in both binary and decimal.*

   Solution There are two approaches:

   Adding in binary, we have

   $$\begin{array}{r} 1\ 1 \\ 10101\text{b} \\ +\qquad 101\text{b} \\ \hline 11010\text{b} \end{array}$$

   Converting this to decimal gives $0 + 2 + 0 + 8 + 16 = 26$.

   Alternatively, we could convert to decimal, then add, then convert back: $10101b = 1 + 4 + 16 = 21$ and $101 = 1 + 4 = 5$. Adding these gives $26 = 16 + 8 + 2 = 11010b$.

5. *Suppose you are given a function $f : \mathbb{N} \to \mathbb{N}$, and are told that $f(1) = 1$ and for all n, $f(n) \leq 2f(\lfloor n/2 \rfloor) + 1$.*

   Use strong induction on n to prove that for all $n \geq 2$, $f(n) \leq 2n \log_2 n$.

   You may write log *to indicate $\log_2$. Here is a reminder of some facts about $\lfloor x \rfloor$ and $\log x$:*

- $\lfloor x \rfloor \leq x$
- $\log 1 = 0$, $\log 2 = 1$
- $\log(x/2) = \log x - 1$
- $\log(2^x) = x$
- $\log(x^2) = 2 \log x$
- *if* $x \leq y$ *then* $\log x \leq \log y$

Solution In the base case, we need to show $f(2) \leq 4 \log 2 = 2$. But we are given that $f(2) \leq 2f(1)+1 = 3 \leq 4$, as required.

For the inductive step, choose $n > 2$, and assume that for all $k < n$, $f(k) \leq 2k \log k$. We must show that $f(n) \leq 2n \log n$.

We compute:

$$\begin{aligned} f(n) &\leq 2f(\lfloor n/2 \rfloor) + 1 && \text{given} \\ &\leq 4\lfloor n/2 \rfloor \log \lfloor n/2 \rfloor + 1 && \text{by inductive hypothesis} \\ &\leq 4(n/2) \log \lfloor (\rfloor n/2) + 1 && \text{by facts stated in question} \\ &\leq 2n \log n - 2n + 1 \leq 2n \log n + (1 - 2n) && \text{arithmetic} \\ &\leq 2n \log n + 0 && \text{since } n > 2 \text{ so } 1 - 2n < 0 \\ &= 2n \log n && \text{as required.} \end{aligned}$$

6. *In this problem, we are working mod 7, i.e.* $\equiv$ *denotes congruence mod 7 and* $[a]$ *is the equivalence of* a *mod 7.*

   (a) *What are the units of* $\mathbb{Z}_7$*? What are their inverses?*

   Solution

   - $[1]$'s inverse is $[1]$
   - $[2]$'s inverse is $[4]$
   - $[3]$'s inverse is $[5]$
   - $[4]$'s inverse is $[2]$
   - $[5]$'s inverse is $[3]$
   - $[6]$'s inverse is $[6]$

   (b) *Compute* $[2]^{393}$.

   Solution $[2]^{393} = ([2]^3)^{131} = [1]^{131} = [1]$

7. *Which of the following sets are countably infinite and which are not countably infinite? Give a one to five sentence justification for your answer.*

   (a) *The set* Σ^* *containing all finite length strings of 0's and 1's.*

   Solution This set is countable. You can list all strings of length 0, then all strings of length one, then all strings of length 2, and so on.

   (b) *The set* $2^{\mathbb{N}}$ *containing all sets of natural numbers.*

Solution This set is not countable. If it were, we could put all of the sets in a table:

	0	1	2	$\cdots$
S_1	$0 \in S_1$	$\notin$	$\in$	$\cdots$
S_2	$\notin$	$\notin$	$\notin$	$\cdots$
S_3	$\in$	$\notin$	$\in$	$\cdots$

We can then construct the set S_D by swapping everything on the diagonal ($S_D = \{i \mid i \notin S_i\}$). Then $S_D \neq S_k$ for any k, because $k \in S_D$ if and only if $k \notin S_k$. Thus S_D is not in the table, which contradicts the fact that the table contained all sets.

(c) *The set* $\mathbb{N} \times \mathbb{N}$ *containing all pairs of natural numbers.*

Solution This set is countable. You can put all of the pairs in a table, and then map the natural numbers to the pairs by tracing diagonals of the table.

(d) *The set* $[\mathbb{N} \to \{0,1\}]$ *containing all functions from* $\mathbb{N}$ *to* $\{0,1\}$*.*

Solution This set is not countable. There is a bijection between $[\mathbb{N} \to \{0,1\}]$ and $2^{\mathbb{N}}$, and we showed above that $2^{\mathbb{N}}$ is uncountable. Alternatively, you can diagonalize directly using the function $f : n \mapsto f_n(n) + 1$ or similar.

Be sure to include enough detail:

- *If listing elements, be sure to clearly state how you are listing them;*
- *If diagonalizing, be sure it is clear what your diagonal construction is;*
- *If providing a function, make sure it is clear what the output is on a given input.*

8. *Use Euler's theorem and repeated squaring to efficiently compute* $8^n \mod 15$ *for* $n = 5$, $n = 81$ *and* $n = 16023$. *Hint: you can solve this problem with 4 multiplications of single digit numbers. Please fully evaluate all expressions for this question (e.g. write 15 instead of* $3 \cdot 5$*).*

Solution We use the fact that $8^{\phi(15)} = 1 \mod 15$. $\phi(15) = (3-1)(5-1) = 8$ [multiplication #1], so we can reduce all of the exponents mod 8. We then use repeated squaring to compute 8^{2^k}:

$$\begin{aligned} [8]^1 &= [8] \\ [8]^2 &= [64] = [4] && \text{[multiplication \#2]} \\ [8]^4 &= [4]^2 = [16] = [1] && \text{[multiplication \#3]} \end{aligned}$$

We can then use these to compute the powers of [8]:

$$\begin{aligned} [8]^5 &= [8]^4[8] = [1][8] = [8] \\ [8]^{81} &= [8]^1 = [8] \\ [8]^{16023} &= [8]^7 = [8]^4[8]^2[8] = [1][4][8] = [32] = [2] && \text{[multiplication \#4]} \end{aligned}$$

9. *For any function* $f : A \to B$ *and a set* $C \subseteq A$, *define* $f(C) = \{f(x) \mid x \in C\}$. *That is,* $f(C)$ *is the set of images of elements of* C. *Prove that if* f *is injective, then* $f(C_1 \cap C_2) = f(C_1) \cap f(C_2)$ *for all* $C_1, C_2 \subseteq A$.

(Hint: *one way to prove this is from the definition of set equality:* $A = B$ *iff* $A \subseteq B$ *and* $B \subseteq A$.)

Solution It's fairly straightforward to prove $f(C_1 \cap C_2) \subseteq f(C_1) \cap f(C_2)$. Consider any $y \in f(C_1 \cap C_2)$. Then $y = f(x)$ for some $x \in C_1 \cap C_2$, which implies that $y \in f(C_1)$ and $y \in f(C_2)$. Hence $y \in f(C_1) \cap f(C_2)$. This direction doesn't rely on the fact that f is injective at all, and is true for all functions.

It's slightly trickier to prove $f(C_1) \cap f(C_2) \subseteq f(C_1 \cap C_2)$. Consider $y \in f(C_1) \cap f(C_2)$. Since $y \in f(C_1)$, there is some $x_1 \in C_1$ such that $f(x_1) = y$. Similarly, since $y \in f(C_2)$, there is some $x_2 \in C_2$ such that $f(x_2) = y$. Therefore $f(x_1) = f(x_2)$. But f is injective, which implies $x_1 = x_2$ (from the definition of injectivity). Hence y is the image of some $x = x_1 = x_2$ in $C_1 \cap C_2$, i.e. $y \in f(C_1 \cap C_2)$.

10. *The Fibonacci numbers $F_0, F_1, F_2, \ldots$ are defined inductively as follows:*

$$\begin{aligned} &F_0 = 1 \\ &F_1 = 1 \\ &F_n = F_{n-1} + F_{n-2} \quad \textit{for } n \geq 2 \end{aligned}$$

That is, each Fibonacci number is the sum of the previous two numbers in the sequence. Prove by induction that for all natural numbers n (including 0):

$$\sum_{i=0}^{n} F_i \ = \ F_{n+2} - 1$$

Solution We will prove this by induction on n. Let $P(n)$ be the statement "$\sum_{i=0}^{n} F_i = F_{n+2} - 1$".

For the base case, we must check that $\sum_{i=0}^{0} F_i = F_1$. This is true (both sides are 1).

For the inductive step, assume the statement is true for some n, that is, $\sum_{i=0}^{n} F_i \ = \ F_{n+2} - 1$. We compute:

$$\begin{aligned} \sum_{i=0}^{n+1} F_i &= \sum_{i=0}^{n} F_i + F_{n+1} \\ &= F_{n+2} - 1 + F_{n+1} && \text{(by the inductive hypothesis)} \\ &= F_{n+1} + F_{n+2} - 1 && \text{(rearranging terms)} \\ &= F_{n+3} - 1 && \text{(from the definition of Fibonacci numbers)} \\ &= F_{(n+1)+2} - 1 \end{aligned}$$

This proves the result for all natural numbers n by induction.

Note: Far too many people provided backwards proofs and were quite heavily penalized as a result. We're sorry, but we've been telling you to avoid this throughout the course. The following proof, which we saw in some version or the other far too often, is **incorrect**.

$$\begin{aligned} \sum_{i=0}^{n+1} F_i &= F_{(n+1)+2} - 1 \\ \sum_{i=0}^{n} F_i + F_{n+1} &= F_{(n+1)+2} - 1 \\ F_{n+2} - 1 + F_{n+1} &= F_{(n+1)+2} - 1 && \text{(by the inductive hypothesis)} \\ F_{n+1} + F_{n+2} - 1 &= F_{(n+1)+2} - 1 && \text{(rearranging terms)} \\ F_{n+3} - 1 &= F_{(n+1)+2} - 1 && \text{(from the definition of Fibonacci numbers)} \\ F_{(n+1)+2} - 1 &= F_{(n+1)+2} - 1 \end{aligned}$$

This is true, so the inductive step is proved, hence the result must be true by induction. QED.

No! No! NOOOOOOOOOOOOOOOOOOOOOOOOOOOO!!!

This proof is backwards. It starts from what you have to prove, and proceeds through a series of implications to a true statement. This does *not* prove the result. (FYI: sure, you may not have put a $\implies$ before each line, but remember we said that that's the default assumption if you omit them. If you wrote $\iff$ or $\impliedby$ before each line, ok, the proof is technically correct and we'll give credit, but it's pretty poor style and difficult to read.)

We don't care if you forget the details of induction and modular arithmetic and graph theory after the course is over (ok we do, a little bit). But we do *really* care if you think backwards proofs are ok. It sets you up badly for all logical reasoning in later life.

It's ok to reason backwards *when working out the problem.* Often that helps you get to the final chain of reasoning more easily. But your proof should work going forwards (from statements known to be true, to the result), and should be presented as such.

11. *Prove by induction that for any integer $n \geq 3$, $n^2 - 7n + 12$ is non-negative.*

Solution Let $P(n)$ be the statement "$n^2 - 7n + 12 \geq 0$". We wish to prove that $\forall n \geq 3, P(n)$. We will prove this by induction.

In the base case, we must show $P(3)$. By inspection, $3^2 - 7 \cdot 3 + 12 = 0 \geq 0$.

Suppose that $P(n)$ holds for some $n \geq 3$. We wish to show $P(n+1)$. We compute

$$\begin{aligned}(n+1)^2 - 7(n+1) + 12 &= n^2 + 2n + 1 - 7n - 7 + 12 \\ &= n^2 - 5n + 6 \\ &= (n^2 - 7n + 12) + (2n - 6) \\ &\geq 0 + 2n - 6 && \text{by } P(n) \\ &\geq 0 && \text{since } n \geq 3\end{aligned}$$

12. (a) *Recall Bézout's identity from the homework: for any integers n and m, there exist integers s and t such that $gcd(n, m) = sn + tm$. Use this to show that if $gcd(k, m) = 1$ then $[k]$ is a unit of $\mathbb{Z}_m$.*

Solution By Bézout's identity, since $gcd(k, m) = 1$, we know that $1 = sk + tm$ for some s and t. Reducing this equation mod m, we find $[1] = [s][k] + [t][m] = [s][k] + [0] = [s][k]$. Therefore, $[k]$ has an inverse, $[s]$, and is thus a unit.

(b) *Use part (a) to show that if p is prime, then $\phi(p) = p - 1$.*

Solution $\phi(p)$ is the number of units mod p. If p is prime, then every number k between 1 and p has $gcd(k, p) = 1$. Therefore, all $p - 1$ non-zero elements of $\mathbb{Z}_p$ are units, so $\phi(p) = p - 1$.

(c) *Use Euler's theorem to compute* $3^{38} \mod 37$ *(note: 37 is prime).*

Solution Since 37 is prime, $\phi(37) = 36$. Therefore, $3^{38} \equiv 3^2 \mod 37$ since $38 \equiv 2 \mod 36$. Thus $3^{38} \mod 37 = 9$.

13. *To disprove $\exists x, \neg\forall y, \neg\exists z, \neg F(x, y, z)$, what would you need to show?*

(a) $\exists x, \exists y, \exists z, F(x, y, z)$

(b) $\exists x, \exists y, \exists z, \neg F(x,y,z)$

(c) $\forall x, \forall y, \forall z, F(x,y,z)$

(d) $\forall x, \forall y, \forall z, \neg F(x,y,z)$

14. $\forall x, \forall y, \forall z, F(x,y,z)$

15.

(a) Write the definition of "$f : A \to B$ is injective" using formal notation ($\forall$, $\exists$, $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $=$, $\neq$, $\dots$).

(b) Similarly, write down the definition of "$f : A \to B$ is surjective".

(c) Write down the definition of "A is countable". You may write "f is surjective" or "f is injective" in your expression. (Note: we gave two slightly different definitions of countable in lecture; we will accept either answer).

Solution

$$\forall y \in B, \exists x \in A, y = f(x)$$

16. Recall that the composition of two functions $f : B \to C$ and $g : A \to B$ is the function $f \circ g : A \to C$ defined as $(f \circ g)(x) = f(g(x))$. Prove that if f and g are both injective, then $f \circ g$ is injective.

Solution [solution 1] From the definition of injectivity, we need to show that if x and y are elements of A and $(f \circ g)(x) = (f \circ g)(y)$, then $x = y$. So we will start by considering any such pair $x, y \in A$ such that $(f \circ g)(x) = (f \circ g)(y)$. Then $f(g(x)) = f(g(y))$ (by definition of composition). Since f is injective, $g(x) = g(y)$. Since g is injective, $x = y$. QED.

[solution 2] Let $h_f : C \to B$ be a left inverse of f and $h_g : B \to A$ be a left inverse of g. These are guaranteed to exist since f and g are assumed to be injective. Now for any $x \in A$, consider $(h_g \circ h_f)((f \circ g)(x)) = h_g(h_f(f(g(x))))$. Since h_f is a left inverse of f, this is equal to $h_g(g(x))$. Since h_g is a left inverse of g, this is equal to x. Hence $h_g \circ h_f$ is a left inverse of $f \circ g$, so the latter must be injective. QED.

17. For each of the following functions, indicate whether the function f is injective, whether it is surjective, and whether it is bijective. Give a one sentence explanation for each answer.

(a) $f : \mathbb{N} \to \mathbb{N}$ *given by* $f : x \to x^2$

Solution injective (no two nonnegative numbers have the same square), not surjective (3 is not in the image), not bijective (since not surjective)

(b) $f : \mathbb{R} \to \mathbb{R}$ *given by* $f : x \to x^2$

Solution not injective ($f(1) = f(-1)$), not surejective (-1 is not in the image), not bijective (not injective, or not surjective)

(c) $f : X \to [Y \to X]$ *given by* $f : x \mapsto h_x$ *where* $h_x : Y \to X$ *is given by* $h_x : y \mapsto x$.

Solution Note: this function always outputs a constant function. If $f(x) = f(x')$ then $x = f(x)(y) = f(x')(y) = x'$ so $x = x'$, thus f is injective.

f is not surjective because it only outputs constant functions, *unless* X has only one element.

It is not bijective because it is not surjective.

18. *A chocolate bar consists of n identical square pieces arranged in an unbroken rectangular grid. For instance, a 12-piece bar might be a 3×4, 2×6 or 1×12 grid. A single snap breaks the bar along a straight line separating the squares, into two smaller rectangular pieces. Prove that regardless of the initial dimensions of the bar, any n-piece bar requires exactly $n - 1$ snaps to break it up into individual squares.*

Solution We will prove this by (strong) induction on n. For the base case, we can use 0 splits to split a one-square candy bar into one square.

For the inductive step, assume the statement holds for all chocolate bars with at most n squares (for some $n \geq 0$), and consider a chocolate bar with $n + 1$ squares. After performing a single split, we are left with two pieces, one of size k (for some $k \leq n$), and one of size $n + 1 - k$ (which is also at most n). By our induction hypothesis, since $k \leq n$, we can split the first piece into one-square pieces using $k - 1$ additional splits. Similarly, we can apply the inductive hypothesis to the second piece to break it into one-square pieces using $n + 1 - k - 1$ splits. In total we have 1 original split, $k - 1$ splits on the first piece, and $n - k$ splits on the second piece, yielding $n = (n + 1) - 1$ splits in total, as required. Hence proved by induction.

Note: Another way to prove this is by induction on the number of rows (or columns) of the bar. This has some caveats you need to be aware of: you have to allow splitting down any row of the bar (not just snap off one row, since you have to prove the result for any pattern of snaps), make sure the statement you're proving (and the base case) is phrased for any number of columns even when you fix the number of rows (e.g. "Claim: a bar with r rows and c columns can be decomposed with $rc - 1$ snaps", and then induct on r), and point out that the proof is general since snaps along columns can be accommodated by rotating the bar by 90°.

19. *Briefly and clearly identify the errors in each of the following proofs:*

    (a) **Proof that 1 is the largest natural number:** *Let n be the largest natural number. Then n^2, being a natural number, is less than or equal to n. Therefore $n^2 - n = n(n-1) \leq 0$. Hence $0 \leq n \leq 1$. Therefore $n = 1$.*

    Solution The error is in the first sentence "Let n be the largest natural number". The proof is only valid *if* there is a largest natural number (which there isn't).

    (b) **Proof that 2 = 1:** *Let $a = b$.*

$$\begin{aligned} \Rightarrow \quad & a^2 = ab \\ \Rightarrow \quad & a^2 - b^2 = ab - b^2 \\ \Rightarrow \quad & (a + b)(a - b) = b(a - b) \\ \Rightarrow \quad & a + b = b \end{aligned}$$

Setting $a = b = 1$, we get 2 = 1.

Solution The error comes when we divide both sides by $(a - b)$, which is zero (division by zero is meaningless!). Just because $(a - b)x = (a - b)y$, we cannot conclude that $x = y$.

(c) **Proof that $(a+b)(a-b) = a^2 - b^2$:**

$$\begin{aligned} \textit{To prove:} \quad (a+b)(a-b) &= a^2 - b^2 \\ \Rightarrow \qquad a^2 - ab + ab - b^2 &= a^2 - b^2 \\ \Rightarrow \qquad a^2 - b^2 &= a^2 - b^2 \end{aligned}$$

. . . which is true, hence the result is proved.

Solution Although the claim is actually true, the proof is backwards; it begins by assuming that the claim is true, and then derives a fact that is known to be true.

This is a valid proof that *if* $(a+b)(a-b) = a^2 - b^2$ *then* $a^2 - b^2 = a^2 - b^2$, but this is not a very interesting fact (and is not what was claimed).

20. *Prove that $7^m - 1$ is divisible by 6 for all positive integers m.*

Solution There are two ways to do this. One way: notice that $7 \equiv 1 \mod 6$, thus $7^m \equiv 1 \mod 6$ for any m (applying the known result that "if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$" $m-1$ times), and thus $7^m - 1 \equiv 0 \mod 6$. This implies $7^m - 1$ is divisible by 6.

Alternatively you can do a direct proof by induction:

Base case: $m = 1$, $7^1 - 1 = 6$ which is obviously divisible by 6.

Inductive step: Assume $7^m - 1$ is divisible by 6 for some $m \geq 1$ (inductive hypothesis). Then $7^{m+1} - 1 = 7^{m+1} - 7 + 6 = 7(7^m - 1) + 6$. But $7^m - 1$ is divisible by 6 (by the inductive hypothesis) and so is 6, so $7^{m+1} - 1$ is also divisible by 6. Hence proved by induction.

21. *Prove that*

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

for all positive integers n.

Solution There is a straightforward proof by induction.

Base case: For $n = 1$, the left-hand side is $\frac{1}{1 \cdot 2}$, and the right-hand side is $\frac{1}{2}$, which are obviously equal.

Inductive step: Assume the statement is true for some $n \geq 1$ (inductive hypothesis). Then

$$\begin{aligned} \sum_{i=1}^{n+1} \frac{1}{i(i+1)} &= \sum_{i=1}^{n} \frac{1}{i(i+1)} + \frac{1}{(n+1)(n+2)} \\ &= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} && \text{(by the inductive hypothesis)} \\ &= \frac{n(n+2)}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} \\ &= \frac{n(n+2)+1}{(n+1)(n+2)} \\ &= \frac{n^2+2n+1}{(n+1)(n+2)} \\ &= \frac{(n+1)^2}{(n+1)(n+2)} \\ &= \frac{n+1}{n+2} \end{aligned}$$

This proves the statement for $n+1$. Hence proved by induction.

Note: We deducted a point for not clearly stating the inductive hypothesis. We also penalized reasoning backwards (the error of 1(c)), even though we let this pass in the prelims, since this has been extensively discussed throughout the course and there is a question in this exam to explicitly warn you against doing this.

There is another neat proof that doesn't require induction. Note that $\frac{1}{i(i+1)} = \frac{1}{i} - \frac{1}{i+1}$. Then the sum can be written as:

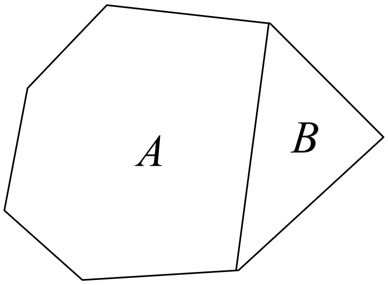
$$\begin{aligned}\sum_{i=1}^{n} \frac{1}{i(i+1)} &= \sum_{i=1}^{n} \left(\frac{1}{i} - \frac{1}{i+1}\right) \\ &= \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{n} - \frac{1}{n+1}\right) \\ &= \frac{1}{1} - \frac{1}{n+1} \qquad \text{(all the other terms cancel out)} \\ &= \frac{n}{n+1}\end{aligned}$$

22. *Prove by induction that the sum of the interior angles of a convex*[1] *polygon with n sides (and hence n vertices) is* $180(n-2)$ *degrees. You may use the fact that the sum of the interior angles of a triangle is 180 degrees. You do not need to prove straightforward geometrical facts rigorously (check with us if unsure).*

Solution The proof rests on the observation that a polygon can be decomposed into two (or more) simpler polygons. Here's one way to do this.

Base case: A triangle is the simplest convex polygon. It has 3 sides and its interior angles sum to 180 = 180 (3 - 2) degrees (given). Hence the base case is true.

Inductive step: Assume that for some n, the interior angles of a convex polygon with n sides sum to $180(n-2)^\circ$. Consider a convex polygon with $n+1$ sides. It can be decomposed into a convex polygon with n sides (A) and a triangle (B) by "chopping off" a vertex.

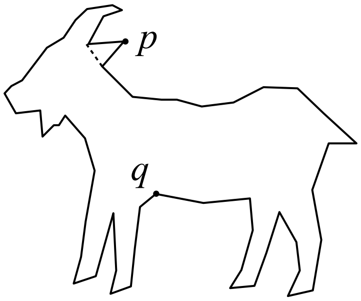


The sum of the interior angles of the $(n+1)$-gon is clearly the sum of the interior angles of A and B. The interior angles of A sum to $180(n-2)^\circ$ (by the inductive hypothesis), and the interior angles of the triangle B sum to 180°. Adding up, we get $180(n-2)+180 = 180(n+1-2)$ degrees, which proves the statement for $n+1$. Hence proved by induction.

Note: There are many other ways to solve this problem, not all of which use induction. For instance, you could use strong induction and break the $(n+1)$-gon into two smaller polygons, neither of which need be a triangle. Or you could pick an arbitrary point in the center of the polygon and draw lines from it to the vertices, splitting the polygon up into n triangles whose interior angles sum to $180n^\circ$, from which you subtract the 360° at the center. This is a correct but non-inductive proof, hence it would not get credit unless you managed to incorporate induction somehow.

[1] A polygon is convex if, for all vertices p and q of the polygon, the line joining p and q lies entirely within the polygon.

For *non*-convex polygons, you can in fact always chop off a triangle (and hence the inductive proof still works), although this is not an obvious result. For instance, in the goat-shaped non-convex polygon below, the "ear" triangle at vertex p can be removed, although no such operation is possible at a different vertex q. This fact leads to a polygon-triangulation algorithm called "ear-clipping".



23. *Suppose that Alice sends the message a to Bob, encrypted using RSA. Suppose that Bob's implementation of RSA is buggy, and computes $k^{-1} \mod 4\phi(m)$ instead of $k^{-1} \mod \phi(m)$. What decrypted message does Bob see? Justify your answer.*

Solution Alice transmits $a^k \mod m$ to Bob, who then computes $(a^k)^{k^{-1}} \mod m$. Because Bob miscomputed k^{-1}, we know that $kk^{-1} \equiv 1 \mod 4\phi(m)$. In other words, $kk^{-1} = 1 + t \cdot 4\phi(m)$ for some t. Therefore Bob receives

$$\begin{aligned}(a^k)^{k^{-1}} &\equiv a^{1+4t\phi(m)} \\ &\equiv a \cdot a^{4t\phi(m)} \\ &\equiv a \cdot (a^{\phi(m)})^{4t} \\ &\equiv a \cdot 1^{4t} \\ &\equiv a \mod m\end{aligned}$$

24. (a) *What are the units of $\mathbb{Z}$ mod 12?*

Solution A unit in a set of numbers is a number that has an inverse. In the set $\mathbb{Z}_{12} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8]$ the units are [1], [5], [7], and [11]. In general, $[n]$ is a unit mod m if n and m are relatively prime.

(b) *What are their inverses?*

Solution $[1]^{-1} = [1]$, $[5]^{-1} = [5]$, $[7]^{-1} = [7]$, and $[11]^{-1} = [11]$. This is because $[1] \cdot [1] = [1]$, $[5] \cdot [5] = [25] = [1]$, $[7] \cdot [7] = [49] = [1]$ and $[11] \cdot [11] = [121] = 1$.

(c) *What is $\phi(12)$?*

Solution By definition of ϕ, $\phi(12)$ is the number of units mod 12. Since there are 4 units, $\phi(12) = 4$.

25. (a) *Let $[X \to Y]$ denote the set of all functions with domain X and codomain Y. Give a function f from $[X \to Y] \times [Y \to Z]$ to $[X \to Z]$.*

Solution Let $f : [X \to Y] \times [Y \to Z] \longrightarrow [X \to Z]$ be given by $f : (g, h) \mapsto h \circ g$. (Recall that $(h \circ g)(x) = h(g(x))$).

Note 1: This is not the only possible function — other solutions are also possible, e.g. the "constant" mapping that returns the same element of $[X \to Z]$ for all input pairs.

Note 2: $g(x), h(x)$ etc are not in general functions! $g(x)$ is the *value* output by g on input x. The function itself is just g. You lost points if you wrote the answer as, for instance, $f : (g, h) \mapsto h(g(x))$ — the RHS is just the value output by the function $h \circ g$ on a particular input x (which is undefined here).

(b) Is your function injective? Is it surjective? Is it bijective?

Solution The function is not surjective in general. For example, if $X = Z = \mathbb{Z}$, but $Y = \{tires\}$, f only outputs constant functions.

The function is not injective either (in general). For example, consider the sets $X = \{Mike, Sid\}$, $Y = \{fermat_{little}, fermat_{last}\}$ and $Z = \mathbb{Z}$. Let $g_1 : X \to Y$ take $Mike$ and Sid both to $fermat_{little}$, and let g_2 take $Mike$ and Sid both to $fermat_{last}$. Similarly, let h take every element of Y to 0. Then $f(g_1, h) = f(g_2, h)$ (these functions both take every element of X to 0), but $(g_1, h) \neq (g_2, h)$.

It is not bijective because it is not injective (also because it is not surjective).

(c) Based on your function, what can you conclude about the relationship between the cardinality of $[X \to Y] \times [Y \to Z]$ and the cardinality of $[X \to Z]$?

Solution This function does not show anything about the relative cardinalities, because it is neither injective nor surjective.